Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
One potential explanation for the website's connection timeout is that the IP address `203.0.113.0` continuously sends TCP SYN packets to the server, attempting to initiate connections without completing the handshake. This behavior results in the server responding with TCP resets. The logs show the server sending: `443 → 32641 [RST, ACK] Seq=0 Win=5792 Len=0` This indicates a possible **SYN flood attack**, where the attacker attempts to exhaust the server's connection queue and resources by initiating — but never completing — a large number of TCP handshakes.

Section 2: Explain how the attack is causing the website to malfunction
When website visitors try to establish a connection with the web server, a three-way handshake must occur using the TCP protocol: 1. **SYN** – the client requests a connection 2. **SYN-ACK** – the server acknowledges and agrees to connect 3. **ACK** – the client confirms the connection In a SYN flood attack, a malicious actor sends a large number of **SYN packets** without ever sending the final ACK. The server keeps these half-open connections in memory, consuming resources. At first, the server attempts to defend itself by sending **RST (Reset)** packets to suspicious or unresponsive connections. However, over time, the volume of

SYN packets overwhelms the server, leading to:

- The server **mistakenly resetting** legitimate user connections
- Eventual **failure to respond** at all (even with RST)

Example log entry:
`443 → 4631 [RST, ACK] Seq=1 Win=5792 Len=0`
This shows the server forcefully ending a connection due to overload — likely affecting a legitimate user.

As a result, real users begin to experience **timeouts**, **gateway errors**, or failure to load web content.